IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA
CHARLESTON

IN THE MATTER OF THE SEARCH OF:

Content of files submitted In connection with CyberTipline Report # 124007236, currently in the custody of Homeland Security Investigations, and more fully described in Attachment A.

CASE NO. 2:22-mj-00068

AFFIDAVIT

Your Affiant, Terrance L. Taylor, having been duly sworn, does hereby depose and state that the following is true to the best of my information, knowledge, and belief:

I. INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge, HSI Charleston, West Virginia. During my career, I gained experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience—including on-the-job discussions with other law enforcement agents and cooperating suspects—I am familiar with the operational techniques and

organizational structure of child pornography distribution networks as well as the traits and characteristics of child pornography collectors and possessors and their use of computers or other electronic and media devices to facilitate the collection, possession, trading, distribution, access and receipt of child pornographic materials.

2. I am a Special Agent with nineteen years of federal law enforcement experience. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, West Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of Inspector General for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center ("FLETC") and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. These areas include laws and regulations pertaining to the importation of various types of merchandise and contraband, prohibited items, money

laundering, and various immigration violations. I have more specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2256.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—file(s) submitted in connection with CyberTipline Report # 124007236 ("the CyberTip"), which are currently in the possession of law enforcement. The files submitted in connection with the CyberTip (more fully described in Attachment A), and the data located therein, there being probable cause to believe that located in the place described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(1), the transportation of child pornography in interstate commerce.

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not

included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(1), the transportation of child pornography in interstate commerce, are located in the place described in Attachment A.

5. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

II. RELEVANT STATUTES

6. The investigation concerns potential violations of 18 U.S.C. §§ 2252A(a)(1), (2), and (5)(B), relating to matters involving the sexual exploitation of minors.

a. 18 U.S.C. 2252A (a)(1) prohibits any person from knowingly mailing, transporting, or shipping child pornography in interest or foreign commerce by any means, including by computer.

b. 18 U.S.C. § 2252A(a)(2) prohibits any person from knowingly receiving or distributing any child pornography that has been mailed or shipped or

transported in interstate or foreign commerce by any means, including by computer.

c. 18 U.S.C § 2252A(a)(5)(B) prohibits any person from knowingly possessing any book, magazines, periodicals films, video tapes computer disk or other matter that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means including computer, or that was produced using materials mailed, or shipped or transported in interstate or foreign commerce by any means including computer.

III. DEFINITIONS

7. The following terms are relevant to this affidavit in support of this application for a search warrant:

a. Child Erotica: The term "child erotica" means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.

b. Child Pornography: The term "child pornography" is defined at 18 U.S.C. § 2256(8). It consists of visual depiction of sexually explicit conduct where

(a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252 and 2256(2), (8).

c. Internet Protocol ("IP") Address: An "IP address" is a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device

every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

d. Minor: The term "minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. Sexually Explicit Conduct: The term "sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

f. Visual Depictions: "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

IV. CYBERTIPLINE REPORT AND PROBABLE CAUSE

8. The National Center for Missing and Exploited Children ("NCMEC") is an organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography.

9. Companies that suspect child pornography has been stored or transmitted on their systems can report that information to NCMEC in a CyberTipline Report ("CyberTip"). To make such a report, a company providing services on the internet, known as an electronic service provider ("ESP") can go to an online portal that NCMEC has set up for the submission of these tips. The ESP, in this case Facebook, can then provide to NCMEC information about the child exploitation activity it believes has occurred, including the incident type, the incident time, any screen or user names associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. Other than the incident type and incident time, the remainder of the information the ESP provides is voluntary and undertaken at the initiative of the reporting ESP. The ESP may also upload to NCMEC any files it collected in connection with the activity. The ESP may or may not independently view the content of the files it uploads.

10. NCMEC does not review the content of these uploaded files not previously viewed by the ESP. Using publicly available search tools, NCMEC attempts to locate where the activity occurred based on the information the ESP provides such as IP addresses. NCMEC packages the information from the ESP along with any additional information it has, such as previous related CyberTips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

11. On or about May 4, 2022, electronic service provider Facebook submitted CyberTipline Report 124007236 to NCMEC. The incident type was identified as apparent child pornography, and the incident time was listed as: May 4, 2022, at 01:20:55 UTC.

12. Facebook also uploaded two files in connection with the report, (1) the profile picture of Facebook user 100076335122631, and (2) an alleged media file of apparent child pornography, the content of which NCMEC did not review. The CyberTipline Report indicated that the ESP did not review the contents of the flagged media file of suspected child pornography: alphanumeric file 6tRekQY1pUSF6bO5279784016_5068884173194981_6307802935936754460_n.mp4. Facebook reported the following additional information: (1) the file at issue was uploaded by Facebook user "Dalo De Jesus" with

user identification number 100076335122631, a date of birth XX-XX-1999, IP address 184.14.110.77, and registered email dalodejesus723@gmail.com. Based on my training and experience, I know that the additional information the ESP provider gave relates to identifiers for the account involved in the incident triggering the CyberTip.

13. NCMEC then used publicly available search tools to discover that the IP address the ESP reported resolved to Frontier Communications. The CyberTip was then provided to law enforcement in this jurisdiction, and I currently have the CyberTip report and the contents of the file that the ESP uploaded in connection with the CyberTip.

14. I know from my training and experience that hash values are widely used by most ESPs and others, including law enforcement, to identify files. A hash value is akin to a fingerprint for a file. A hash value is obtained by processing the contents of a file through a cryptographic algorithm, which produces a unique numerical value—the hash value—that identifies the unique contents of the file. If the contents of the file are modified in any way the value of the hash will also change. I know from my training and experience that the chances of two files with different content having the same hash value are infinitesimal.

15. I know from my training and experience that many ESPs compare the hash values of files that its customers transmit on its systems against a database containing hash values of known child pornography material. If the ESP finds that a hash value on its system matches one in the database, the ESP captures the file along with information about the user who uploaded, posted, possessed, or otherwise transmitted the file on the ESP's systems. This information is then transmitted to NCMEC in the form of a CyberTipline Report.

16. The image file at issue here, alphanumeric file 6tRekQY1pUSF6bO5279784016_5068884173194981_630780293593675 4460_n.mp4, was flagged by the ESP based on a hash match.

17. Based on information contained in the CyberTipline Report, it appears that Facebook did not independently review any of the material submitted in connection with the CyberTip. Although Facebook did not review this material, I have probable cause to believe the material contains child pornography, by virtue of the hash match to a database of known child pornography. The CyberTipline Report categorized the image file as a pubescent minor engaged in a lascivious exhibition. The CyberTipline Report clarified that "lascivious exhibition" is "Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus

on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value."

18. In summary, there is probable cause to believe that the material Facebook sent to NCMEC in connection with the CyberTipline Report contains child pornography, including any material that may not have been previously reviewed by Facebook.

V. INTERSTATE NEXUS

19. I submit that the element of "in or affecting interstate or foreign commerce" is satisfied for a violation of 18 U.S.C. § 2252A, for the limited purpose of securing a search warrant, through use of the ESP servers and use of the Internet in connection with this offense.

VI. CONCLUSION

20. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that inside the file that Facebook uploaded in connection with the above Cybertip 124007236 (described in Attachment A), evidence, fruits, and instrumentalities of violations of Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography; 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(1), (described in

Attachment B) will be found.

21. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items described in Attachment A, for the items listed in Attachment B.

I swear that this information is true and correct to the best of my knowledge.

SPECIAL AGENT TERRANCE L. TAYLOR
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

SUBSCRIBED and SWORN to before me by telephonic means this 27th day of May, 2022.

DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE

2:22-mj-00068

ATTACHMENT A

Description of property and location to be searched

Content of files uploaded in connection with CyberTipline Report #124007236 (hereinafter and in Attachment B the "File(s)"), currently held securely by Homeland Security Investigations at 210 Kanawha Boulevard West, Charleston, WV 25302.

ATTACHMENT B

Description of Items to Be Seized and Searched

For the File(s) listed and described in Attachment A, the following items, that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), (2), and (5)(B):

1. Visual depictions of child pornography, including image or video files.
2. Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors.
3. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the File(s), or that aid in the identification of persons involved in violations of 18 U.S.C. §§ 2252A(a)(1), (2), and (5)(B).

DEFINITIONS:

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer data or electronic storage; any handmade form (such as writing, drawing, painting); any mechanical form (such as printing

or typing); and any photographic form (such as digital image files; microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).